PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059323
(43)Date of publication of application : 25.02.2000

(51)Int.Cl. H04H 1/00
H04L 9/08
H04L 9/10
H04L 29/08
H04N 7/167

(21)Application number : 10-224825
(22)Date of filing : 07.08.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NISHIMURA TAKUYA
IIZUKA HIROYUKI
YAMADA MASAZUMI
GOTO SHOICHI
TAKECHI HIDEAKI
USUKI NAOJI

(30)Priority

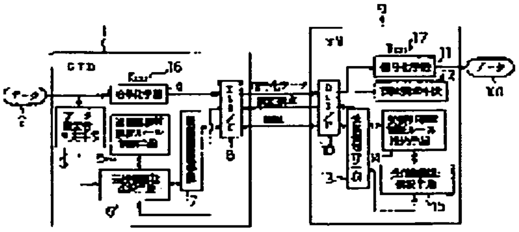
Priority number :	Priority date :	Priority country :
10031847	13.02.1998	JP
10151586	01.06.1998	JP

(54) DIGITAL AV DATA TRANSMISSION UNIT, DIGITAL AV DATA RECEPTION UNIT, DIGITAL AV DATA TRANSMISSION/RECEPTION SYSTEM AND MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To appropriately perform data communication while being immune to forgery or alteration and considering the importance of data or class of a recognition method by receiving an authentication request and performing authentication based on one kind of authentication rule selected out of a means storing plural authentication rules on the side of transmission based on the discriminated result of a data importance discriminating means.

SOLUTION: When an authentication requesting means 12 receives the authentication request, a data importance discriminating means 3 discriminates the importance of AV data 2 to be transmitted and classifies them according to CGMS values. A transmission side authentication selecting means 6 sends the optimum authentication rule, which is selected out of a means 5 storing plural authentication rules on the side of transmission, to a digital AV reception unit TV9. At a digital AV transmission unit STB1, the same authentication rule as the selected certification rule is selected and a reception side authentication means 13 and a transmission side authentication means 7 mutually perform the



authentication. When the authentication is made successful, the AV data 2 to be transmitted are enciphered and transmitted while using a work key Kco16 and the received enciphered data are deciphered by a work key Kco17.

LEGAL STATUS

[Date of request for examination]	16.08.2001
[Date of sending the examiner's decision of rejection]	17.12.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	2003-00846
[Date of requesting appeal against examiner's decision of rejection]	14.01.2003
[Date of extinction of right]	

[0041] First, authentication request unit 12, which composes digital AV data reception unit TV9, sends out an authentication request, including its own ID, to digital AV data transmission unit STB1 through digital interface D-I/F10. Of course an AV data transmission request is also sent out. Digital AV data transmission unit STB1 receives the authentication request through digital interface D-I/F8. Then the digital AV data transmission unit STB1 determines the importance of AV data 2, which must be sent at data importance determination unit 3, and performs processing on the data. In other words, in the case where the value of CGMS is 11, the importance level is high, and the data may only be displayed, copying is prohibited. In the case where the CGMS value is 10, the data can be copied only once and is comparatively important data. In the case where the CGMS is 00, the data may be viewed, copied and used freely, and so it could be said that it is not important data. Likewise, there is no AV data with a CGMS value of 01. The data importance is determined and processing performed according to the value of the CGMS. The result is sent to the authentication selection unit 6 on the transmission side and the best authentication rule is selected from the plural authentication rule storage unit 5 on the transmission side. In other words, for important data like the latest movies and so on, although time-consuming, an authentication rule utilizing a public key and a private key strong to forgery or interference will be selected. Meanwhile, for unimportant data like news, an authentication rule weak to forgery or interference which is not time-consuming and utilizes a common key will be selected. Further, the selection information is sent to authentication unit 7 on the transmission side and to digital AV reception unit TV 9 through digital interface D-1/F8. In digital AV reception unit TV 9, authentication selection unit 15 on the receiving side selects, utilizing the selection information, the same authentication rule as the authentication rule chosen by digital AV data transmission unit STB1, from plural authentication rule storage unit 14 on the receiving side. Consequently, the chosen authentication rule becomes the same for the transmission side and the receiving side. Thus, authentication unit 13 on the receiving side and authentication unit 7 on the transmission side mutually perform authentication through digital interface D-I/F10 and digital interface D-I/F8. Once authentication is successful, a work key Kco 16 for the transmission side and a work key Kco 17 for the receiving side will be generated as mentioned later. Data 2, which must be sent, is encrypted at encryption unit 4 utilizing the generated work key Kco 16. Afterwards, data 2 is sent as encrypted data through digital interface D-I/F8 to digital AV data reception unit TV9. The encrypted data through digital interface D-I/F10 is decrypted at decryption unit 11 using work key Kco 17 and becomes a data

101. This is identical to data 2 and the data is sent to digital AV data reception unit TV 9 from digital AV data transmission unit STB1.

[0042] Lastly, digital AV data reception unit TV9 displays the data in the display screen of the display device. In this way, when the data importance is high, an authentication method strong to forgery or interference are utilized, though this method is time-consuming; likewise, when the data importance is low, a non-time-consuming authentication rule weak to forgery or interference is utilized.

[0043] Next, the authentication exchange is shown as above for when an authentication request is sent out from digital AV data reception unit TV9 to digital broadcast unit STB1, and thereby the embodiment that generates work key Kco as its result is introduced with reference to FIG.4 and FIG.5.

[0044] To begin with as shown in FIG.4, a case of performing authentication by public and private keys: In this case the receiving side has private key Sb and public key Pb. The transmission side has private key Sa and public key Pa. In step 1, the receiving side first generates random number B. The receiving side sends its own identification number IDb and random number B, as well as cryptograph Sb (B), encrypted by its own private key Sb, to the transmission side. The transmission side acquires the public key Pb of the receiving side by searching based on the identification number IDb of the receiving side. Cryptograph Sb(B) is decrypted by using the public key Pb acquired in step 8. As a result, a random number B is obtained according to step 9. Further, on the receiving side a random number A is generated according to step 10. Random numbers A and B are encrypted by private key Sa on the transmission side and a cryptograph Sa (A, B) is created. The receiving side receives cryptograph Sa (A, B) and an identification number IDa of the transmission side. The receiving side obtains the public key Pa of the transmission side by searching based on the identification number IDa of the transmission side, and as in step 2, decodes cryptograph Sa (A, B) with Pa. Here, a random number B identical to the random number B sent in step 1 is obtained by the receiving side and the receiving side ascertains that no forgery or interference has been carried out. If it happens that the two random numbers differ, it is ascertained that forgery or interference has been carried out and that there is an unauthorized peer. However, in this case it is supposed that public key Pa, Pb are only obtainable by an authorized party. Next, just like in step 3, random number A is encrypted by secret key Sb of the receiving side and cryptograph Sb (A) is created. Sb (A) is sent to the transmission side and cryptograph Sb (A) is decrypted by public key Pb on the receiving side, which the transmission side already possesses as in step 11. When the random number B generated in step 10 and the random number B decrypted in step 11 are identical, the transmission side will ascertain that no forgery or interference is being carried out. When the two values differ, it will be ascertained that forgery or interference has been carried out and that there is an unauthorized peer.

[0045] Now supposing that forgery or interference has not been carried out with the random numbers A and B exchanged between the receiving side and the transmission side, random numbers A and B are secret random numbers to any third parties outside of the receiving side and transmission side. Accordingly, a key Kab is created on the transmission side using random number A and B, as in step 12. In the same way a key Kab is created on the receiving side as in step 4 using random number A and B. The two Kab will be identical and will be common keys. Next, a key Kex is created on the transmission side as in step 13. This is encrypted by common key Kab, and a cryptograph Kab (Kex) is created and sent to the receiving side. The receiving side decrypts cryptograph Kab (Kex) with common key Kab as in step 5, so as to obtain Kex; as a result, key Kex obtained by the receiving side is identical with the key Kex on the transmission side and becomes a common key. Next a key Kco is created on the transmission side as in step 14. Key Kco is encrypted by common key Kex and, as a cryptograph Kex (Kco), is sent to the receiving side. On the receiving side, cryptograph Kex (Kco) is decrypted with common key Kex as in step 6 and Kco is obtained as in step 7. Since the key Kco on the transmission side and the Kco on the receiving side are identical, they are a common key. The above is work key Kco obtained in the authentication process by a public key and a secret key.

[0046] Next, authentication by a common key will be presented as in FIG.5. In this case, the transmission and receiving sides possess common key S. Note that this common key is given only to authorized parties. First, two random numbers A1 and A2 are generated as in step 15, encrypted by common key S, creating a cryptograph S (A1A2) which is sent to the transmission side. On the transmission side, cryptograph S (A1A2) is decrypted by common key S as in step 20. Thus random numbers A1 and A2 are obtained as in step 21. The transmission side sends random number A2 to the receiving side. The receiving side comes to possess the two random numbers A1 and A2 as in step 16. When the random number A2 generated in step 15 and the random number A2 received from the transmission side in step 16 are identical, it is ascertained on the transmission side that forgery or interference are not being carried out. Were the above two random numbers to differ, authentication would fail because forgery or interference had been carried out. Next, the transmitting side generates random numbers B1 and B2 as in step 22, encrypts, and sends cryptograph S (B1B2) to the receiving side. The receiving side decrypts cryptograph S (B1B2) using common key S as in step 17. Upon which random numbers B1 and B2 are obtained as in step 18. The receiving side sends random number B2 to the transmission side. The transmission side comes to possess random numbers B1 and B2 as in step 23. When the random number generated in step 22 and the random number B2 received from the receiving side in step 23 are identical, it is ascertained by the receiving side that no forgery or interference has been being carried out and authentication succeeds. Were the above two numbers to differ, authentication would fail because forgery or interference had been carried out.

[0047] When authentication has succeeded to this point, random number A1 and random number B1 are secret random numbers from third parties outside of the transmission side and the receiving side. On the transmission side, key Kco is created from random number A1 and random number B1 as in step 24. On the receiving side, key Kco is created from random number A1 and random number B1 as in step 19. Key Kco on the transmission side and key Kco on the receiving side are identical and are a common key. The above is work key Kco, obtained from the authentication process with a common key.

[0048] Note that in the present invention, the types of authentication rules selected are not limited to the above two types of authentication rules, that is, the one using a public key and a secret key and the other using a common key, and further, more than three different types of authentication rules may be used.